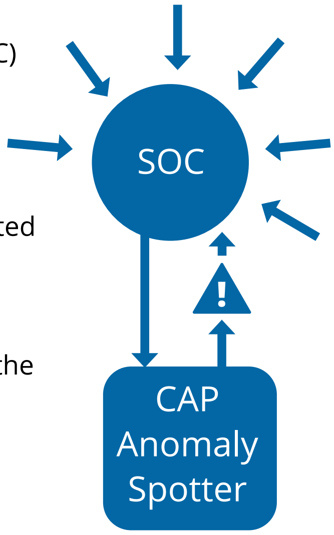
CAP ANOMALY SPOTTER

Anomaly Detection for Security Operation Centers and MSSPs

In enterprise IT security, Security Operation Center (SOC) is a dedicated unit that monitors, assesses and defends enterprise information systems, such as web sites, applications, databases, data centers and servers, networks, desktops and other endpoints. SOCs may be operated by the enterprises themselves, or by a dedicated security service provider, so called MSSP (Managed Security Service Provider).

The technology platform of a SOC is typically based on the SIEM (Security information and event management) approach. SIEM is a technology solution that "aggregates event data produced by security devices, network infrastructures, systems, and applications." (Gartner)



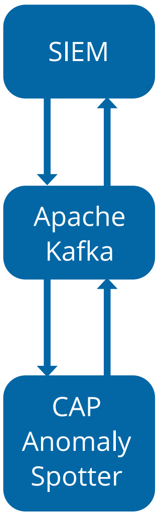
Opportunity for advanced machine learning analytics in SIEM

The core capabilities of SIEM systems are event collection with a broad scope and ability to correlate, analyze them and ability to visualize the situational image. While all SIEM systems provide these main functionalities, core value comes from the analytical intelligence of the system. Therefore SIEM providers and their customers are continuously looking for more advanced analytical technologies to upgrade the system. According to a user survey (SANS, 2015), the most desired feature for security managers is integrating more end-point related intelligence, upgrading SIEMs with analytics to catch unknown indicators, i.e., anomaly detection.

Case: CAP Anomaly Spotter for SIEM

Company: IT security service company

The challenge: Our customer is a MSSP providing outsourced device and system security monitoring and management to their enterprise customers.They were looking for an anomaly detection solution to upgrade their SIEM platform. The core requirement was to identify unusual patterns and behavior in the data collected from the target system.



Our solution: We adopted CAP Anomaly Spotter engine to the specific use cases. CAP integrates to the SIEM platform using Apache Kafka or another similar message broker as the modular interfacing component between the underlying SIEM infrastructure and the CAP Anomaly Spotter engine. The solution is cost-effective, modular, and flexible. CAP module is installed to our customer's systems as a Docker container. The SIEM system collects data from various sources from the enterprise network. Apache Kafka sends the data to CAP Anomaly Spotter in a pre-defined format. CAP Anomaly Spotter conducts the machine learning operation in parallel to the basic SIEM functionalities. CAP component sends back the results through the same channel and the results are incorporated to the main functionalities and to the user interface.

Benefits of CAP Anomaly Spotter

- Detects and highlights the most noteworthy anomalous events and incidents using advanced machine learning analytics.
- Improves efficiency and decreases the cost of SOC operations by automating the detection of the most noteworthy events in the system.
- Improves reactiveness to security threats and system failures.
- Modular integration to the SIEM platform is cost-effective and flexible. CAP Anomaly Spotter operates in parallel, and does not affect the performance of the SIEM functionalities.

About CAP Data Technologies

CAP Data Technologies is a Finnish technology startup providing data analytics solutions utilizing our advanced anomaly detection technology. CAP Anomaly Spotter has the ability to detect previously unknown behavior in the system without relying on pre-set rules or fingerprints.

Contact CAP Data Technologies

tuomo.sipola@capdatatechnologies.com tel: +358 40 753 2169
markku.ranta@capdatatechnologies.com tel: +358 50 324 6233

Try out the free trial version on our web site
www.capdatatechnologies.com